Cybersecurity provisioning for Industry 4.0 digital twin with AR components*

Ruslan Kozak[1,†], Yuriy Skorenkyy[1,*,†], Oleksandr Kramar[1,†], Taras Lechachenko[1,†] and Halyna Brevus[1,†]

[1] *Ternopil Ivan Puluj National Technical University, 56 Ruska St, Ternopil, UA46001, Ukraine*

Abstract

Threat model for Industry 4.0 enterprise data platform is built within STRIDE model with use of the TODIM method and intuitionistic fuzzy sets. Processes and data types relevant for a smart manufacturing have been analyzed to build the specific threat model. The security controls and mitigation actions have been identified, the respective threats and vulnerabilities were systematized for the industrial data platform design with AR-enhanced digital twin of the production equipment. The implementation of additional security controls to address the extended attack surface for industrial data platforms will facilitate the prioritization of the proposed countermeasures and mitigation actions.

Keywords

Industrial Data Platform, Augmented Reality, Cybersecurity, Threat Modeling

1. Introduction

The digital transformation of Ukrainian enterprises is a pressing imperative, underscored by the potential integration into the European Community and the advantages proffered by the unified European market. However, this transition is not without its complexities and necessitates a comprehensive consideration of various risks, particularly those affecting the security of industrial infrastructures and their workforce [1, 2].

Adopting the Industry 4.0 paradigm necessitates the aggregation and analysis of data across all facets of the manufacturing cycle to facilitate real-time decision-making, avert crises, and prevent equipment malfunctions [3, 4]. Such data emerges as a pivotal asset, warranting robust safeguards against cyber threats and other nefarious activities. Unauthorized intrusions can precipitate not only the forfeiture of proprietary industrial data and sensitive information but also the interruption of manufacturing operations, degradation of product quality, and tangible hazards to the personnel overseeing the machinery [5, 6].

In the realm of transformative technologies that are reshaping production, Augmented Reality (AR) and Virtual Reality (VR) are particularly noteworthy [7-10]. While the digitization inherent to the Industry 4.0 model yields direct benefits, the deployment of AR interfaces introduces vulnerabilities associated with the employment of personal gadgets, such as tablets and smartphones, within the industrial digital framework [11]. Concurrently, these instruments, in tandem with the data amassed in the production environment, potentially can enhance the physical safety protocols within the enterprise [12].

This study focuses on the approach to industrial data platform development that prioritizes cybersecurity, benefiting manufacturers who implement smart manufacturing, and emphasizes the

* *CITI'2025: 3rd International Workshop on Computer Information Technologies in Industry 4.0, June 11–12, 2025, Ternopil, Ukraine*

1* Corresponding author.

† These authors contributed equally.

ruslan.o.kozak@gmail.com (R. Kozak); skorenkyy@tntu.edu.ua (Yu. Skorenkyy); kramar_o@tntu.edu.ua (O. Kramar); taras5a@ukr.net (T. Lechachenko); h.kravchuk@tntu.edu.ua (H. Brevus)

0000-0003-1323-6448 (R. Kozak); 0000-0002-4809-9025 (Yu. Skorenkyy); 0000-0003-0805-3732 (O. Kramar); 0000-0003-1185-6448 (T. Lechachenko); 0009-0009-5614-0241 (H. Brevus)

importance of implementing effective techniques at the organizational level while recognizing the significance of policy implications in promoting widespread adoption [13, 14]. The proposed approach for integrating cybersecurity aspects into the design of AR-enabled digital twin (DT) will help address issues of data integration in the metal processing industry. Widespread adoption of digital platforms with AR tools may contribute to novel collaborative business models promoting sustainable development.

2. Related works

An important aspect of Internet of Things (IoT) is the possibility of developing hybrid solutions that can combine physical products with digital services, particularly through mobile devices. Modern smartphones not only act as an intermediary between people [15], physical, and digital entities [11] but also allow accumulating valuable information about the cognitive, emotional, and behavioral patterns of the user, which can eventually be used to develop alternative IoT devices, particularly with the use of mixed reality. One of the main technologies to facilitate human integration into such a system is AR, which provides an interface [16, 17] for people to interact with the digital world of smart manufacturing.

A basic property of AR technology that can be used for smart manufacturing is a tracking system that allows accurately placing digital models of objects in the physical reality [18]. It is easiest to implement the AR tracking technology based on physical markers localized in certain places of industrial lines or installations and used to determine the correct position of digital images. However, degradation of markers over time or poor lighting can significantly hinder marker recognition. Therefore, natural markers are often used, without any physical objects superimposed on the real assets to specify the position of virtual objects. Wider implementation of AR technology will bring benefits to assistance in assembly operations in smart production, training of engineering experts, creation of a navigation system for operators, logistics warehouse operations, maintenance production nodes, product quality control, etc. (see [7, 19] for an overview).

In case of the appearance of atypical scenarios of equipment operation or malfunctions of individual nodes, the elimination of such malfunctions becomes a rather difficult and time-consuming process, as it requires access to specific information, and their filtering and selection, which is quite time-consuming. The augmented reality layer, which provides well-structured information in real-time in a specific location, has significant potential for visualization and contextualization of data, allowing optimization of the decision-making process of the maintenance operator with the help of remote services [19, 20]. Using AR, personnel can practice various scenarios safely in a controlled interactive way. Failures of the equipment can be simulated in the immersive environment to allow covering not just technical but also psychological aspects. Development methodologies such as human-centered design can ensure improvement of personnel skills and knowledge in the workplace, with safe and efficient AR training and upskilling [19].

The STRIDE methodology is a widely recognized approach for identifying and mitigating threats in software systems [21]. It was developed by Microsoft and covers different categories of threats (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege). In comparison with other threat modeling methodologies, STRIDE is relatively simple and easy to understand, making it a popular choice, especially for less experienced security practitioners [22, 23]. However, its simplicity can also be seen as a limitation, as it may overlook more complex or specific threats that don't fit neatly into the STRIDE categories. One of the most well-known alternative methodologies is PASTA (Process for Attack Simulation and Threat Analysis), which is a risk-based approach that considers both technical and business impact factors [24]. PASTA is generally considered more comprehensive than STRIDE, but it is also more complex and resource-intensive to implement. LINDDUN (Linkability, Identifiability, Nonrepudiation, Detectability, Disclosure of information, Unawareness, Noncompliance) is more focused on privacy protection [25]. Another popular methodology is OCTAVE (Operationally Critical Threat, Asset,

and Vulnerability Evaluation), which is a risk-based approach developed by Carnegie Mellon University. OCTAVE is focused on identifying and prioritizing information assets based on their criticality to the organization [26]. It is often used in conjunction with other methodologies, such as STRIDE, to provide a more holistic view of risks. In contrast to these risk-based approaches, methodologies like VAST (Visual, Agile, and Simple Threat) focus more on the attack surface and potential attack vectors [27]. These methodologies can be useful for identifying specific vulnerabilities but may not provide a comprehensive view of the overall risk landscape.

While each methodology has its strengths and weaknesses, the choice ultimately depends on the specific needs and resources of the organization. In practice, many organizations adopt a hybrid approach, combining elements of different methodologies to create a tailored threat modeling process [22].

3. Cybersecurity threat modeling approach

Digitization of manufacturing, being a prerequisite for efficient collaboration in production clusters of Industry 4.0 enterprises, laid the foundation for industrial data exchange within the value chains. One may distinguish between different levels of information exchange which involve principally different cyber security challenges and threats [28, 29]. In this study, we model the industrial ecosystem as a hierarchy of three levels, namely intra-enterprise industrial data platform [9, 10], inter-enterprise data exchange and comprehensive data ecosystem for clusters of enterprises from the economy sector [30], like the European Factory Platform.

The provision of a robust cybersecurity framework necessitates the characterization of the nature of data and the associated data sources [31]. This paper examines a specific use case of an enterprise deploying a digital twin integrated with an extended reality interface. The digital twin of a manufacturing line enables management to control the production in real-time, increases production efficiency, ensures better maintenance of individual production units by implementing predictive maintenance practices, and flexibly reconfigure the production when needed [32]. The main production operations, covered by the production model and the corresponding digital twin of the chosen use-case, are plasma and laser cutting, automatic welding, bending, and powder coating. In addition, micro-logistics within production, quality control, and product labeling should be included in the process model.

Since the working equipment of the production line poses threats to the physical safety of workers, the hardware is to be equipped with IoT measuring devices that will work autonomously and transmit relevant and accurate information in real-time about both the quality of product components and the technical condition of the equipment [3]. Data flows into the digital twin originate from measurements carried out at the production equipment. Measurements are conducted on milling machines (to control shape and size using a camera and laser distance meters), in an internal production silo (to count the number and characterize the assortment of workpieces according to weight and size characteristics), after welding with a Kuka robot (to control the welding seams using multi-spectral images and conductivity probes), after the correcting press (by compliance with the template or by laser distance meter data), and after painting the product (by recognizing the image). Compliance of the entire complex of measured characteristics with the technological map of production is a necessary condition for high product quality. Timely receipt of accurate data (classified in Table 1) on the workload of production line nodes can allow flexible sharing of certain nodes (for example, a welding robot) by several production chains [33].

Table 1
Data types, relevant for the industrial data platform

Decision-making level	Production process level	Data type
Production data	Production process data	Parts consumption data IoT sensors' data Waste production data
	Equipment status data	Configuration data Operating mode data
	Service data	Maintenance data Service reports
Energy consumption data	Grid electricity consumption data	Power Seasonal variations
Environmental data	Factory data Surrounding area data	Temperature Humidity Noise and air pollution

The diagram in Figure 1 illustrates architecture for the ecosystem of industrial data platforms governed by digital twins, which aims to create a virtual representation of a physical production environment [34]. It depicts the various components involved, such as factory floor, consisting of production equipment, IoT sensors and actuators; digital twin of the physical assets and processes, comprising models and industrial data infrastructure; interfaces for human-machine interaction (with an augmented reality processor for visualizing and interacting with the digital twin) and machine-machine interactions (for cybersecurity reasons it is desirable to separate industrial data machine-machine interface from software support interface), internal enterprise database and external industrial knowledge bases (repositories for storing and managing data, rules, and insights derived from the digital twins, for use by the entire economy sector). Users may be internal or external, including all stakeholders who leverage the digital twin and knowledge base for decision-making, such as operators, management, regulatory bodies, and emergency services.

4. Cybersecurity threat model for Industry 4.0 Digital Platform

For the cyber security purposes, threat modeling is used as a method to identify security requirements and, on this basis, single out system vulnerabilities and security threats. The subsequent prioritization of protective measures requires a comprehensive assessment of impact and severity of those threats. This procedure is applied to software and computer networks, including IoT components which control the production life-cycle. Industrial data platforms specified by Figure 1 can be protected using the STRIDE [21] methodology for threat modeling identifying its vulnerabilities and characteristic security threats. Within this methodology, data flow diagram and the threat model have been developed (see Figure 2) for the industrial ecosystem based on enabler technologies described in works [35, 36].

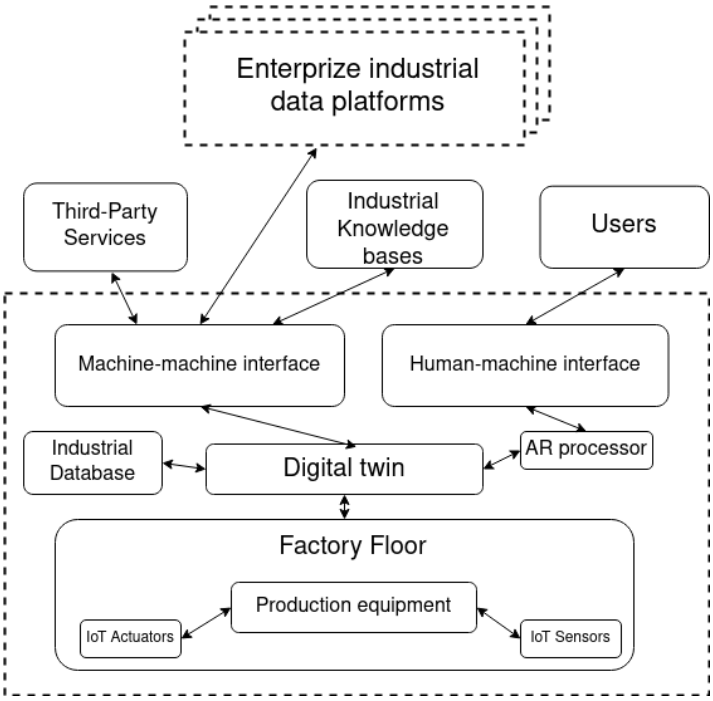

Figure 1: Representation of the industrial ecosystem and components of an individual production facility data platform.

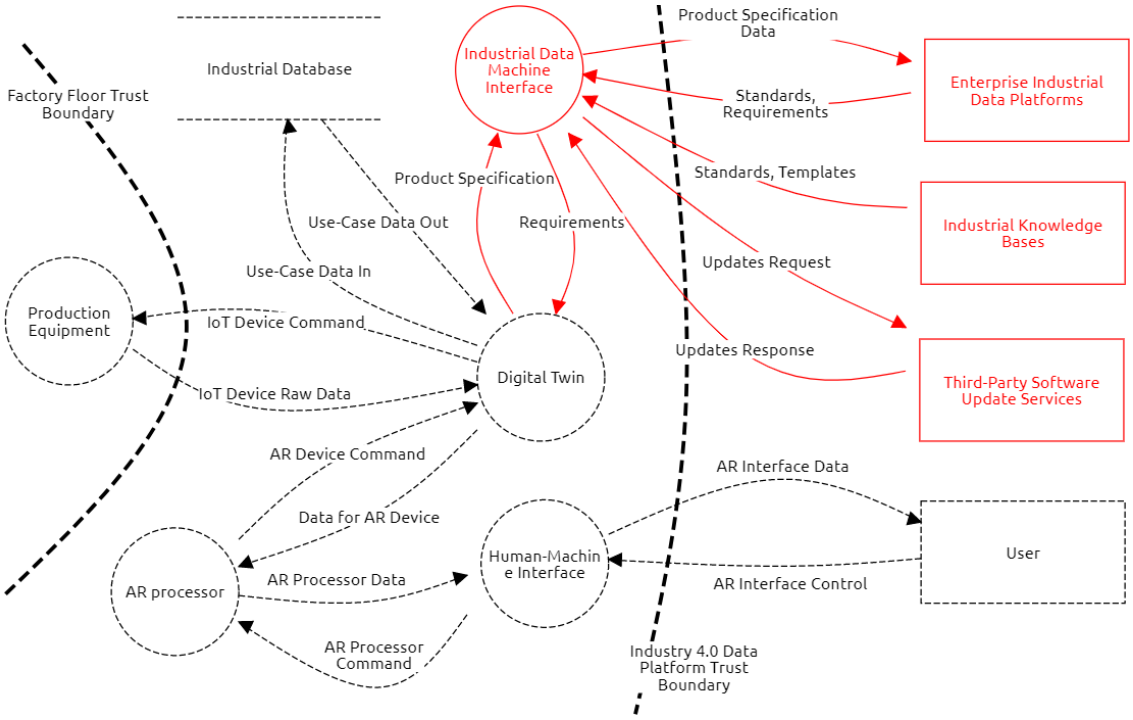

Figure 2: Data flow diagram for the considered Industry 4.0 Data Platform architecture.

In Figure 2 a group of elements which may become part of the extended attack surfaces is identified (those elements are shown in red). This is a peculiar property of systems with the embedded IoT components of the industrial data platform. Security threats and risks of their realization were assessed in the assumption that modern visualization and control technologies are integrated into the digital twin.

In Table 2 the identified security threats and the corresponding mitigation measures are listed, according to the STRIDE methodology. The proposed measures may be implemented both in the processes of design of Industry 4.0 ecosystems and during security audits for improvement of

existing ones. The selected groups of elements from the data flow diagram (Figure 2) have their corresponding threats and specific countermeasures, that are meticulously chosen from those defined in Open Web Application Security Project (OWASP) Internet of Things Top Ten [37]. This allows also to select tests for evaluation of attack surfaces for the industrial data platform and the corresponding vulnerabilities [38-41].

For the considered industrial data platform the OWASP IoT Top Ten has been adapted, security practices and security controls have been proposed for effective mitigation of critical threats that may hamper the platform operation.

It should be stressed that the left-shift approach to cybersecurity during design, implementation and utilization of Industry 4.0 platforms is to be applied to efficiently block cyber-attacks and reliably protect the sensitive data assets.

The implementation of additional security controls to address the extended attack surface for industrial data platforms will facilitate the prioritization of the proposed countermeasures and mitigation actions [39].

Table 2
Security threats and countermeasures for the designed industrial data platform

Type of Security threat	The component for which the threat is analyzed	Proposed countermeasures
Spoofing (claiming a false identity)	Industrial Data Machine Interface, Enterprise Industrial Data Platforms, Industrial Knowledge Bases, Third-Party Software Update Services	Encryption usage, Strong cryptographic protocols: PGP, AES, SHA-2, TLS 1.2 / 1.3, Strong authentication mechanisms: MFA, biometric auth, certificate pinning, OAuth
Tampering (malicious modifications of data or process)	Industrial Data Machine Interface, Product Specification / Requirements, Product Specification Data, Standards, Requirements, Updates Response / Updates Request, Standards, Templates	Security Labeling, Secure communication protocols, Proper authorization mechanisms, Data hashing and signing
Repudiation (denial of taking an action or recognizing an event occurrence)	Industrial Data Machine Interface, Enterprise Industrial Data Platforms, Industrial Knowledge Bases, Third-Party Software Update Services	Logging and audit trails
Information Disclosure (leakage of the sensitive data)	Industrial Data Machine Interface, Product Specification / Requirements, Product Specification Data, Standards, Requirements, Updates Response / Updates Request, Standards, Templates	Proper authorization mechanisms, Encryption usage, Strong cryptographic protocols: PGP, AES, SHA-2, TLS 1.2 / 1.3, Secure coding best practices
Denial of Service (unavailability of an asset, service or network resource for purposive users)	Industrial Data Machine Interface, Product Specification / Requirements, Product Specification Data, Standards, Requirements, Updates Response / Updates Request, Standards, Templates	Antimalware software, Security applications, Redundancy
Elevation of Privilege (gaining unauthorized access or privileges)	Industrial Data Machine Interface	Proper authorization mechanisms, Principles of least privilege, Logging and audit trails, Access certification

5. Multi-criteria decision making based on TODIM method

The components identified in the data flow diagram (Figure 2) were ranked according to the STRIDE threat model using the TODIM (an acronym for Tomada de Decisão Interativa Multicriterio, meaning Interactive Multi-criteria Decision Making) method [42, 25] and intuitionistic fuzzy sets [43]. Three experts from cross-functional teams with more than five years of experience in cybersecurity and human-machine interfaces were interviewed to collect raw data for the TODIM method implementation.

The experts were tasked to assess the potential damage to the Industry 4.0 platform by evaluating the impact of various threats on each component within the framework of the given scenario:

- Spoofing: malicious actors could spoof identities to gain access to manufacturing systems or IoT devices, disrupting automated workflows or injecting false data.
- Tampering: attackers might modify sensor data in real-time monitoring or interfere with programmable logic controllers, leading to incorrect decision-making and operational failures.
- Repudiation: insiders could deny responsibility for malicious activities, resulting in making forensic analysis difficult after security incidents.
- Information Disclosure: leaked process optimization algorithms or proprietary design files could harm competitiveness and expose vulnerabilities.
- Denial of Service: DoS attacks on smart factory networks or cloud-based manufacturing solutions could halt production, impair predictive analytics, and disrupt supply chain.
- Elevation of Privilege: attackers could escalate their privileges within Industry 4.0 components to manipulate cyber-physical systems, disable security mechanisms, or alter manufacturing parameters.

A linguistic variable scale described by Table 3 has been used. To facilitate this process, the linguistic variables from the ranking scale referenced in paper [44] were adapted, and the modified scale specified in Table 3 was utilized.

Table 3
Intuitionistic linguistic variables

Linguistic term	IFNs
Critical Impact (CI)	[1.00; 0.00; 0.00]
High Impact (HI)	[0.85; 0,05; 0.10]
Medium-High Impact (MHI)	[0.70; 0.20; 0.10]
Medium Impact (MI)	[0.50; 0.50; 0.00]
Low-Medium Impact (LMI)	[0.40; 0.50; 0.10]
Low Impact (LI)	[0.25; 0.60; 0.15]
Miserable Impact (Msl)	[0.00; 0.90; 0.10]

Distribution of the experts' evaluations (Figures 3, 4) can be easily explained by the fact that experts' opinions are based on their extensive expertise in the field of cybersecurity where, indeed, data tampering, spoofing and denial of service cause immediate and severe disruptions. The collected set of expert evaluations allows us to overcome an existing problem of the absence of the relevant data in the literature, as companies are reluctant to share details about cybersecurity breaches, damaging to their reputation. At the same time, one may expect slight correction of

numerical data for elevation of privileges and repudiation, which, however, will not change the priorities for mitigation actions.

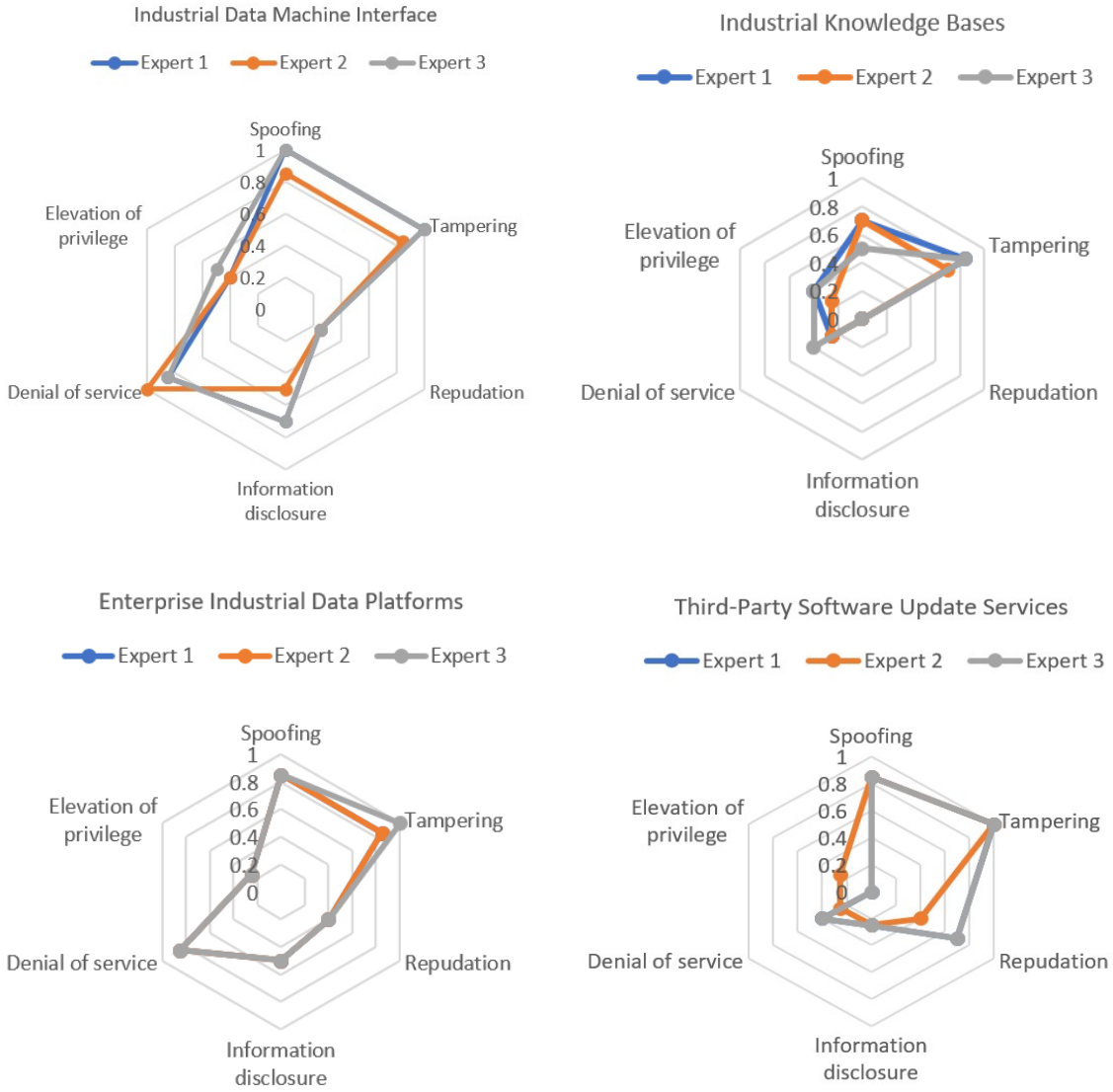

Figure 3: Comparison of scores deviation for experts' evaluations of components.

Worth noting, for the data flows we have reduced the subset of threats analyzed in STRIDE model, as some of those threats are relevant only to the objects like digital twin or data platform. This peculiarity does not allow neglecting the cybersecurity provisions focused specifically on the data exchange. Instead, mitigation measures are to be designed according to the principles of shared responsibility and may have multi-tier structure, starting from cyber defense of the objects external with respect to the industrial data platform (the external industrial platforms, third party services) and culminating at inner objects (digital twin, machine interfaces).

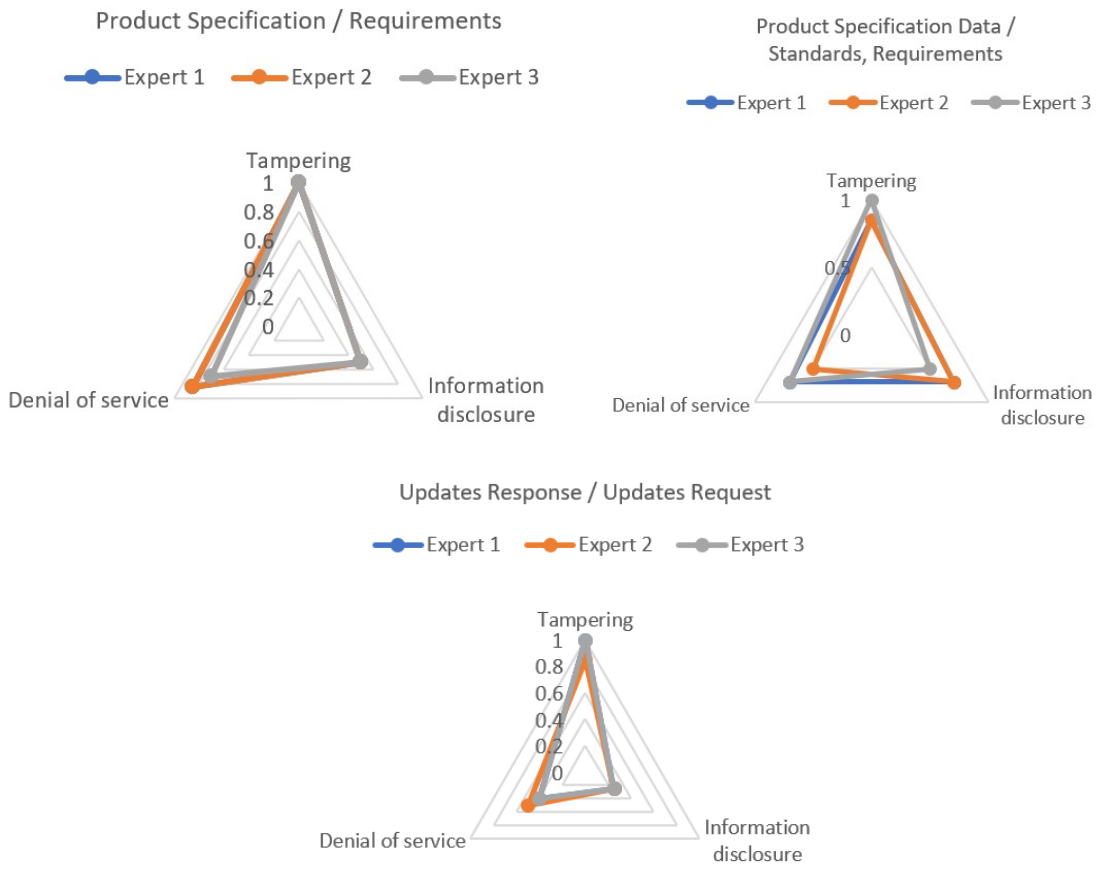

Figure 4: Comparison of scores deviation for experts' evaluations of data flows.

The fuzzy intuitionistic evaluations of the experts were aggregated using the formula provided in source [44]:

$$d_{ij}=IFW\ Ar_{\lambda}\left(r_{ij}^{(1)},r_{ij}^{(2)},\ldots,r_{ij}^{(k)}\right)=\lambda_1 r_{ij}^{(1)},\lambda_2 r_{ij}^{(2)},\ldots,\lambda_k r_{ij}^{(k)}=\left[1-\prod_{l=1}^{k}\left(1-\mu_{ij}^{l}\right)^{\lambda_l},\prod_{l=1}^{k}\right. \quad (1)$$

Here, $r_{ij}^{(k)}$ denotes the evaluation of the i- assessment by the k-expert according to the j criterion, the value λ_k - indicates the corresponding expert's weight, while μ_{ij}^{l}, $v_{ij}^{(l)}$represent fuzzy intuitionistic values.

The metric for calculating the distance between intuitionistic fuzzy numbers A and B is applied as outlined in [45]:

$$d_H(A,B)=\frac{1}{2n}\sum_{i=1}^{n}\left(\left|\mu_A(x_i)-\mu_B(x_i)\right|+\left|v_A(x_i)-v_B(x_i)\right|+\left|\pi_A(x_i)-\pi_B(x_i)\right|\right) \quad (2)$$

The TODIM method [24] has the following algorithm. For a set of alternatives $\{a_1,a_2,\ldots a_m\}$ be, and a set of criteria, $\{c_1,c_2,\ldots c_n\}$ with normalized weights $\{w_1,w_2,\ldots w_n\}$. A matrix $a=\left[d_{ij}\right]_{m\times n}$ is constructed, where d_{ij} represents the evaluation of alternative $a_i(i=1,2,\ldots m)$ based on criterion $c_j(j=1,2,\ldots n)$. Assume that $w_{jk}=w_j/w_k$ are the relative weights for each criterion c_j , c_t where $w_k=max(w_j)\quad k,j=1,2\ldots,n$. Then the TODIM method is applied as follows:

1. Normalization $a = \left[d_{ij} \right]_{m \times x}$ into $a' = \left[d'_{ij} \right]_{m \times x}$ is performed.

2. Calculation of a dominance for alternative a_i over alternative a_t is done based on criterion c_j, considering the factor ρ as a mitigating factor for loss effects. Thus, the calculation is as follows:

$$\delta(a_i, a_t) = \sum_{j=1}^{n} \upsilon_j(a_i, a_t)(i,t = 1,2...,m)$$

$$\upsilon_j(a_i, a_t) = \begin{cases} \sqrt{w_{ik}(d_{ij} - d_{tj}) / \sum_{j=1}^{n} w_{jk}} & if\ d_{ij} - d_{tj} > 0 \\ 0 & if\ d_{ij} - d_{tj} = 0 \\ -\frac{1}{\rho}\sqrt{(\sum_{j=1}^{n} w_{jk})(d_{ij} - d_{tj}) / w_{jk}} & if\ d_{ij} - d_{tj} < 0 \end{cases} \quad (3)$$

$\upsilon_j(a_i, a_t)(d_{ij} - d_{tj} > 0)$ corresponds to an advantage and $\upsilon_j(a_i, a_t)(d_{ij} - d_{tj} < 0)$ characterizes a loss. The factor ρ is considered to be the mitigating factor for loss effects.

3. The overall evaluation is obtained by the formula:

$$\delta(a_i) = \frac{\sum_{t=1}^{m} \delta(a_i, a_t) - min\left\{ \sum_{1}^{m} \delta(a_i, a_t) \right\}}{max\left\{ \sum_{1}^{m} \delta(a_i, a_t) \right\} - min\left\{ \sum_{1}^{m} \delta(a_t, a_t) \right\}} \quad (4)$$

4. The best alternative has the greatest value of $\delta(a_i)$.

Table 4
TODIM ranking of components for the designed industrial data platform

Name of component	Coefficient	Position
Industrial Data Machine Interface	1	1
Enterprise Industrial Data Platforms	0.82	2
Third-Party Software Update Services	0.49	3
Product Specification Data / Standards, Requirements	0.34	4
Product Specification / Requirements	0.31	5
Updates Response / Updates Request	0.05	6
Industrial Knowledge Bases	0	7

Table 4 presents the ranking of AR-enabled Digital Twin system components based on STRIDE threats, as assessed using the TODIM method. The ranking results highlight the need for significant efforts within the secure-by-design approach, particularly focusing on the process components of the IDT architecture and their corresponding security controls and mitigations.

Comprehensive implementation of the TODIM method in the framework of STRIDE model allows us to quantify the evaluations made by cybersecurity experts. In this way we reduce

possible biases which could impact decision making and support the process of secure-by-design development of digital twins for Industry 4.0 enterprises.
Besides the final numerical results, visual dashboards representing distribution of the expert evaluations (see Figures 3, 4) deserve to be included into the process of decision making. Firstly, these dashboards help develop intuitive understanding of the different inherent vulnerabilities of a complex Industry 4.0 data platform architecture. Secondly, areas inside the net diagram allows to qualitatively compare the necessary resources for the efficient cyber defense of the particular digital asset or data exchange mechanism.

Conclusions

Aggregation of various data in Industry 4.0 ecosystems offers rich possibilities for production optimization and product improvements. At the same time, implementation of digital twins to steer and virtualize manufacturing extends the cyber-attack surfaces of industrial data platforms. A secure-by-design approach is to be strictly followed to protect valuable data and the enterprise infrastructure.

A threat model for an industrial data platform, proposed in the present work, allows to identify and analyze specific groups of objects and data flows to devise efficient measures for cyber protection. For an Industry 4.0 enterprise which leverages its digital assets and implements advanced AR tools, full awareness of the extended attack surfaces is a prerequisite for efficient cyber defense. Based on STRIDE methodology, one may perform efficient prioritization of vulnerabilities and choose the best mitigation actions to optimize the design and support the improvement of industrial data platforms and their components.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] A. Malatras, Ch. Skouloudi, A. Koukounas. Industry 4.0 - Cybersecurity Challenges and Recommendations. European Union Agency for Network and Information Security (ENISA), 2019.

[2] E.Avdibasic, S. Amanzholova, B. Durakovic. Cybersecurity challenges in Industry 4.0: A state of the art review. Defense and Security Studies 3 (2022): 32-49.

[3] L.D. Xu, E.L. Xu, and L. Ling. Industry 4.0: state of the art and future trends. International journal of production research 56, no. 8 (2018): 2941-2962. DOI: 10.1080/00207543.2018.1444806.

[4] J. Pochmara, A. Świetlicka. Cybersecurity of Industrial Systems—A 2023 Report. Electronics 13, no. 7 (2024): 1191. DOI: 10.3390/electronics13071191.

[5] M. Dawson. Cyber security in industry 4.0: The pitfalls of having hyperconnected systems. Journal of Strategic Management Studies 10, no. 1 (2018): 19-28. DOI: 10.24760/iasme.10.1_19.

[6] M. Nankya, R. Chataut, R. Akl. Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies. Sensors 23, no. 21 (2023): 8840. DOI: 10.3390/s23218840.

[7] J. Egger, T. Masood. Augmented reality in support of intelligent manufacturing–a systematic literature review. Computers & Industrial Engineering 140 (2020): 106195. DOI: 10.1016/j.cie.2019.106195.

[8] Chan Qiu, Shien Zhou, Zhenyu Liu, Qi Gao, Jianrong Tan. Digital assembly technology based on augmented reality and digital twins: a review. Virtual Reality & Intelligent Hardware 1, no. 6 (2019): 597-610. DOI: 10.1016/j.vrih.2019.10.002.

[9] Y. Skorenkyy, R. Zolotyy, S. Fedak, O. Kramar, R. Kozak. Digital Twin Implementation in Transition of Smart Manufacturing to Industry 5.0 Practices. CEUR Workshop Proceedings 3468 (2023): 12–23.
[10] S. Fedak, Y. Skorenkyy, M. Dautaj, R. Zolotyy, O. Kramar. Digital Twins for Optimisation of Industry 5.0 Smart Manufacturing Facilities. CEUR Workshop Proceedings, 3628, (2023): 344–349.
[11] D. Mourtzis, J. Angelopoulos, N. Panopoulos. Operator 5.0: A survey on enabling technologies and a framework for digital manufacturing based on extended reality. Journal of Machine Engineering 22 (2022). DOI: 10.36897/jme/147160.
[12] A. Bécue, E. Maia, L. Feeken, P. Borchers, I. Praça. A new concept of digital twin supporting optimization and resilience of factories of the future. Applied Sciences 10, no. 13 (2020): 4482. DOI:10.3390/app10134482.
[13] T.H. Khan, Chiho Noh, Soonhung Han. Correspondence measure: a review for the digital twin standardization. The International Journal of Advanced Manufacturing Technology 128, no. 5-6 (2023): 1907-1927. DOI: 10.1007/s00170-023-12019-3.
[14] H. Nahorniak, A. Sverstiuk. Transformation of intellectual capital into intellectual-information in the process of formation and implementation modern information. CEUR Workshop Proceedings 3039 (2021): 335 – 352.
[15] A. Ilic, E. Fleisch. Augmented Reality and the Internet of Things. Auto-ID Labs White Paper WP-BIZAPP-068: 2016. DOI: 10.3929/ethz-a-010833302.
[16] O. Kramar, Y. Drohobytskiy, Y. Skorenkyy, O. Rokitskyi, N. Kunanets, V. Pasichnyk, O. Matsiuk. "Augmented Reality-assisted Cyber-Physical Systems of Smart University Campus." In 2020 IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT), vol. 2, pp. 309-313. IEEE, 2020.
[17] T. Kramar, O. Duda, O. Kramar, O. Rokitskyi, V. Pasichnyk. Peculiarities of Augmented Reality Usage in a Mobile Application: The Case of Ivan Puluj Digital Museum. CEUR Workshop Proceedings, 3309, (2022): 279-287.
[18] J. Novak-Marcincin, J. Barna, M. Janak, L. Novakova-Marcincinova. Augmented reality aided manufacturing. Procedia Computer Science 25 (2013): 23-31. DOI: 10.1016/j.procs.2013.11.004.
[19] T. Masood, J. Egger. Augmented reality in support of Industry 4.0—Implementation challenges and success factors. Robotics and Computer-Integrated Manufacturing 58 (2019): 181-195. DOI: 10.1016/j.rcim.2019.02.003.
[20] D. Mourtzis, V. Siatras, J. Angelopoulos. Real-time remote maintenance support based on augmented reality (AR). Applied Sciences 10, no. 5 (2020): 1855. DOI: 10.3390/app10051855.
[21] R. Khan, K. McLaughlin, D. Laverty, S. Sezer. "STRIDE-based threat modeling for cyber-physical systems." In 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe) IEEE. (2017): 1-6. DOI: 10.1109/ISGTEurope.2017.8260283.
[22] A. Shostack. Threat modeling: Designing for security. John Wiley & Sons. 624p. 2014. ISBN: 978-1-118-80999-0.
[23] N. Shevchenko. Evaluating Threat-Modeling Methods for Cyber-Physical Systems. Carnegie Mellon University, Software Engineering Institute's Insights (blog) (2019), Accessed April 24, 2024, https://insights.sei.cmu.edu/blog/evaluating-threat-modeling-methods-for-cyber-physical-systems/.
[24] T. UcedaVelez, M.M. Morana. Risk Centric Threat Modeling: process for attack simulation and threat analysis. John Wiley & Sons, 2015. ISBN 978-0-470-50096-5.
[25] K. Wuyts, D. van Landuyt, A. Hovsepyan, W. Joosen. "Effective and efficient privacy threat modeling through domain refinements." In Proceedings of the 33rd Annual ACM Symposium on Applied Computing. (2018): 1175-1178. DOI: 10.1145/3167132.3167414.
[26] B. Tucker, Advancing Risk Management Capability Using the OCTAVE FORTE Process. Software Engineering Institute. 2020. DOI: 10.1184/R1/13014266.v1.

[27] N.R. Mead, F. Shull, K. Vemuru, O. Villadsen. "A hybrid threat modeling method." Carnegie MellonUniversity-Software Engineering Institute-Technical Report-CMU/SEI-2018-TN-002 (2018). http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=516617

[28] N. Tuptuk, S. Hailes. Security of smart manufacturing systems. Journal of manufacturing systems 47 (2018): 93-106. DOI: 10.1016/j.jmsy.2018.04.007.

[29] O. Nakonechnyi, A. Pashko, A. Sverstuik, I. Shevchuk. Statistical Simulation of the External Influence of the Information Spreading of the Population Models. 2020 IEEE 2nd International Conference on System Analysis and Intelligent Computing, SAIC 2020 (2020): 9239225. DOI: 10.1109/SAIC51296.2020.9239225.

[30] N. Anumbe, C. Saidy, R. Harik. A Primer on the Factories of the Future. Sensors 22, no. 15 (2022): 5834. DOI: 10.3390/s22155834.

[31] A. Corallo, M. Lazoi, M. Lezzi, P. Pontrandolfo. Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level. IEEE Transactions on Engineering Management. vol. 70. no. 11,(2023): pp. 3745-3765. DOI:10.1109/TEM.2021.3084687.

[32] Fei Tao, Qinglin Qi, Ang Liu, A. Kusiak. Data-driven smart manufacturing. Journal of Manufacturing Systems 48 (2018): 157-169. DOI:10.1016/j.jmsy.2018.01.006.

[33] Ray Zhong, Xun Xu, E. Klotz, S.T. Newman. Intelligent manufacturing in the context of industry 4.0: a review. Engineering 3, no. 5 (2017): 616-630. DOI: 10.1016/J.ENG.2017.05.015.

[34] S. Boschert, R. Rosen. Digital twin—the simulation aspect. Mechatronic futures: Challenges and solutions for mechatronic systems and their designers (2016): 59-74. DOI: 10.1007/978-3-319-32156-1_5.

[35] P.K.R. Maddikunta, Quoc-Viet Pham, B. Prabadevi, N. Deepa, K. Dev, T.R. Gadekallu, R. Ruby, M. Liyanage. Industry 5.0: A survey on enabling technologies and potential applications. Journal of Industrial Information Integration 26 (2022): 100257. DOI: 10.1016/j.jii.2021.100257.

[36] Y. Drohobytskiy, V. Brevus, Y. Skorenkyy. "Spark structured streaming: Customizing kafka stream processing." In 2020 IEEE Third International Conference on Data Stream Mining & Processing, pp. 296-299. IEEE, 2020.

[37] OWASP (Open Web Application Security Project). OWASP Internet of Things Project. 2018. https://owasp.org/www-project-internet-of-things/.

[38] G. Lally, D. Sgandurra. "Towards a framework for testing the security of IoT devices consistently." In Emerging Technologies for Authorization and Authentication: First International Workshop, ETAA 2018, Barcelona, Spain, September 7, 2018, Proceedings 1, pp. 88-102. Springer International Publishing, 2018. DOI: 10.1007/978-3-030-04372-8_8.

[39] T. Lechachenko, T. Gancarczyk, T. Lobur, A. Postoliuk. Cybersecurity Assessments Based on Combining TODIM Method and STRIDE Model for Learning Management Systems. CEUR Workshop Proceedings, 3468, (2023): 250-256.

[40] T. Lechachenko, R. Kozak, Y. Skorenkyy, O. Kramar, O. Karelina, Cybersecurity Aspects of Smart Manufacturing Transition to Industry 5.0 Model, CEUR Workshop Proceedings 3628, (2023): 325-329.

[41] V. Martsenyuk, A. Sverstiuk, O. Bahrii-Zaiats, Y. Rudyak, B. Shelestovskyi. Software complex in the study of the mathematical model of cyber-physical systems. CEUR Workshop Proceedings 2762 (2020): 87–97.

[42] J. Wang, G. Wei, M. Lu, TODIM Method for Multiple Attribute Group Decision Making under 2-Tuple Linguistic Neutrosophic Environment. Symmetry 10 (2018) 486. DOI: 10.1080/17509653.2017.1349625.

[43] K.T. Atanassov, Intuitionistic fuzzy sets. Physica-Verlag HD. 1999. 1- 137.

[44] B.D. Rouyendegh, The Intuitionistic Fuzzy ELECTRE model, International Journal of Management Science and Engineering Management, 13:2 (2018) 139-145. DOI: 10.1080/17509653.2017.1349625.

[45] E. Szmidt, J. Kacprzyk. Distances between intuitionistic fuzzy sets. Fuzzy sets and systems 114.3 (2000): 505-518. doi.org/10.1016/S0165-0114(98)00244-9